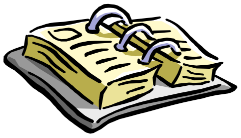
MESSENGER
THE PRESCOTT COMPUTER SOCIETY'S NEWSLETTER - PRESCOTT, ARIZONA

# November 2016

Visit our website at www.pcs4me.com Ken Johnson, Newsletter Editor



## CALENDAR

SIG = Special Interest Group

### This Week's Schedule

**November 12 - Saturday - 1:10-2:50 PM**
General Meeting - Leader: Phil Ball
Location: Prescott Public Library; Founders Suite A & B

First Hour: **"Stump the Geeks!"**

Yes - it's time to have another "Stump the Geeks" session. Plan on bringing your computer and smartphone questions to the meeting and our panel will do their best to answer them. As with many meetings at the Library, this session is expected to be unusually unpredictable so there should be a high entertainment value as well as being educational.

Second Hour: Phil Ball will present Tips and Tricks with insights into various topics that assist with regular computer activity.

**In addition to the presentations, the following are typical events which take place at our General meetings:**

1) *We hold an informal Flea Market in which you are encouraged to bring in your excess computer equipment or software and make them available for others to enjoy at no charge. Please deposit give-away items on the table in the back marked "Free Stuff." Any items left here at the end of the meeting are subject to disposal.*

*2) If you have items that are just too good to give away, you may set up a separate table and hold your own sale.*
*3) We conduct a raffle of gift cards at the end of the meeting, so make sure to get a pair of tickets from whoever is in charge and place one on the item you'd like to win.*
*4) We will also accept your used ink and toner cartridges for recycling. They are turned in to Think4Inc for credits which PCS uses to purchase office supplies from them.*

2) **Future Meetings:November 19 - Saturday - 1:10-2:50 PM**
Special Topics SIG - Leader: JB Burke
Location: Prescott Public Library; Founders Suite A & B
This month, JB will delve into topics related to computer hardware, software, the Internet and the World Wide Web. You are sure to find something educational and/or entertaining and/or interesting in

Calendar *Cont on Pg 2*

## Future Meetings, continued:

this fastpaced enjoyable session. As always, questions and comments will be welcome. After all, JB has to be learning something from these sessions too!

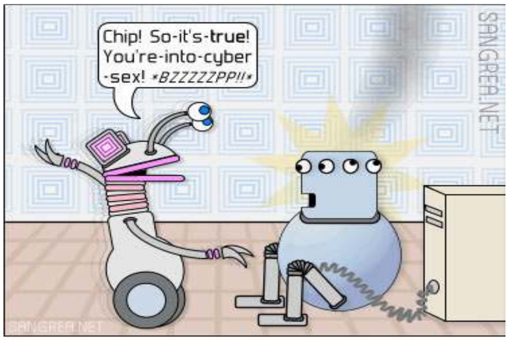
**November 26 - Saturday**
There will be no PCS meeting today.

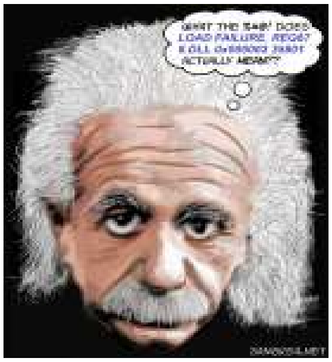
*Note that these dates are correct at time of publication but are subject to change.*
*Up to date information can be found on our website, www.pcs4me.com*

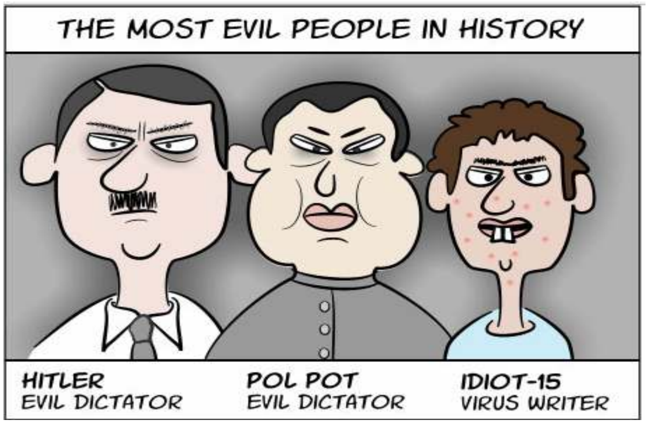
*Unless otherwise noted, our meetings are usually held in the*
*Founder's Suite at the Prescott Public Library.*

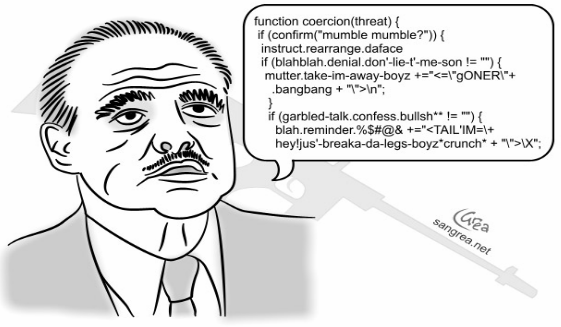
## Prescott Computer Society
## Officers & Board of Directors
## 2015-2016

| Officers: | | General Directors: | |
|---|---|---|---|
| President | Ray Carlson | Joan Baum | Murray Smolens |
| Vice Pres | Phil Ball | John Carter | Dick Mason |
| Secretary | JB Burke | Ken Johnson | |
| Treasurer | Edi Taylor-Richards | | |









```
function coercion(threat) {
 if (confirm("mumble mumble?")) {
  instruct.rearrange.daface
  if (blahblah.denial.don'-lie-t'-me-son != "") {
   mutter.take-im-away-boyz +="<=\"gONER\"+
     .bangbang + "\">\n";
    }
   if (garbled-talk.confess.bullsh** != "") {
     blah.reminder.%$#@& +="<TAIL'IM=\+
     hey!jus'-breaka-da-legs-boyz*crunch* + "\">\X";
```

The Godfather's biggest contribution to society
was inspiring the development of encryption

*Continued on pg 3*

# Computer Attacks

By Dick Maybach, Member, Brookdale Computer Users' Group, NJ

June 2016 issue, BUG Bytes
www.bcug.com

An important factor in defending your computer is to understand how it might be attacked. This topic fascinates many computer owners and has been the subject of many articles, books, advertisements, and discussions. One result of this is a jumble of terminology with words having meanings almost as slippery as the programs they are trying to describe. In this article I'll attempt to untie the terminology knot with brief definitions of the most common terms. You can learn (much) more with an Internet search for any of these terms, provided you read with skepticism. We'll start by using **attack** to describe any malicious act directed at a computer, the data it contains, or its user. We can classify attacks in three different ways:

(1) their **attack method** (how they access your PC, your data, or you),

(2) their **behavior** (how they get established and perhaps spread), and

(3) their **payload** (what they do).

To a great extent, these characteristics are independent, and we can look at each in turn. Much of the confusion about malware arises because authors don't make it clear whether what they are describing is an attack method, a behavior, or a payload.

First consider network attacks, which may not affect your computer at all. The first type, **network monitoring** is passive and is a digital version of a phone tap; everything you send and receive is recorded by a third party. This is easily done at a public hot spot, and requires only a laptop and widely-available software. It also can occur at ISPs and Internet relay points, either by the facility owner or by government agencies. A second type, the **man in the middle** attack, is active and is much more specific. Here, a computer is set up to mimic, for example, your Internet bank. If you can be fooled into logging into it, the attacker can capture your password and other account details before forwarding your traffic to the bank site you think you are using. This is more difficult to set up than simple network monitoring and is thus less common.

Let's now look at computer attack methods, which Include:

(1) physical access,
(2) social engineering,
(3) Trojan horses, and unethical suppliers.

Someone with **physical access** to your PC can install malicious hardware or software. Although this is sometimes called the **evil maid** attack (presumably because it's done by a hotel's housekeeping staff), it more commonly occurs when someone uses your PC with your permission and inadvertently infects it during, for example, a careless Internet browse. You now have a compromised PC for such tasks as your Internet banking. **Social engineering** or **phishing** occurs when someone tries to convince you to disclose sensitive data or perform some action that compromises your computer. You might receive a phone call or an e-mail message claiming to be from your credit card company requesting your account information, or one from tech support offering to remove a virus they somehow have detected remotely. Many attacks occur as **Trojan horses**, where malevolent software hides inside something that appears useful, interesting, or at least harmless. Examples include e-mail (often appearing to be from somebody you know) with an attachment that installs software, Web pages that run programs on your PC, and macros embedded in office files. Finally, there are **unethical suppliers** that include software you neither need nor want with their products. Although the most common culprits are Websites, it can take the form of **shovelware**, useless and sometimes intrusive programs installed on PCs, and malicious software on supposedly blank media.

Once **malware** (which malicious software is often called) infects your PC, it can behave in four different ways:

(1) reside there as a normal program file,
(2) attempt to hide by changing its form or the operating system configuration,
(3) spread through your computer by attaching a portion of itself to other files or
(4)send copies of itself to other computers, usually via the Internet.

Type (2) programs are called **stealth software** or **rootkits**, type (3) programs are called **viruses**,

*Continued on pg 4*

Continued from pg 3:

form of virus resides in office document as a **macro**, for example written in Visual Basic and cluded in an MS Word or Excel file. These can migrate to your master template and infect every document you compose after that. When they first appeared around 2000 macro viruses were serious problems, but office suites now have effective safeguards against most; however, you may wish to check your preferences to be sure. (Although many people use the term virus for all malware, only 17 per cent of it really behaves this way and another eight per cent acts as worms.) Combinations are also possible; for example, a virus can have stealth features. Since rootkits and viruses can affect system programs, their installation often, but not always, requires that the user grant them administrator privileges. A number of vendors offer applications to detect rootkits, but removing one sometimes requires erasing the computer's hard drive and reinstalling the operating system. Many people call type (1) programs Trojan horses, but I prefer to use that term for a malicious program's attack method rather than it's behavior after it becomes active.

Note that network attacks, social engineering, and macro viruses are operating-system agnostic. OS X and Linux users are just as vulnerable to them as are Windows users.

The object of most malware is to deliver a payload that is to perform some action to harm the computer owner or benefit the malware supplier. The payload is independent of the attack method and also of the malware's behavior. Examples are:

(1) ransomware,
(2) adware,
(3) spyware,
(4) key loggers,
(5) botnets, and
(6) hijackers.

**Ransomware** restricts your access to your PC and displays a message on how you can purchase instructions or software to remove the limitation. In some cases it encrypts files and demands the fee in return for the password to regain access to them. Sometimes there is just a threat, such as pay a fee within 10 days or your hard disk will be formatted. **Adware** continually displays advertising messages on your screen, although this can be legitimate (if annoying) when it's associated with trial software and seeks to sell you the paid version. **Spyware** transmits sensitive information, such as account information and passwords to an Internet location without your permission. Some people lump adware and spyware together and call both spyware, but I prefer to keep them separate, since spyware is more costly. A **key logger** records your keystrokes and forwards them to n Internet location with the intent of capturing log-in information; it can be implemented by either hardware or software. Malware can make your PC a component of a **botnet** (also called a zombie army), a computer network sometimes used to distribute spam or to attack other Internet sites by trying to overwhelm them. Other payloads, having a variety of names that often include the term **hijack**, change the configuration of your browser by changing your home page or your search engine or by adding menu bars.

By far the best time to defend your computer is in the attack phase, where healthy suspicion is your friend. Be careful reading e-mail, surfing the Internet, and using your laptop in public places. Note that some form of social engineering is a component of most attacks. After the attack, an anti-virus program may be able to recognize the malware's behavior and prevent it from delivering its payload. Here, you depend on the malware spreading relatively slowly, so that anti-virus vendors have had time to develop a defense before you encounter it, and fortunately this is most often the case. Once the payload has been delivered, the damage has been done, and you will have to stop using the computer until it can be cleaned, change your passwords, and work with your bank, credit card vendors, and others to repair the damage.

We usually think of malware defense only for PCs, but it also infects all computer-driven devices, such as smart phones and network routers. It's important that you include these in your safe computing plan.

Your ultimate defense against all malware is a backup made before your PC became infected. Wiping and restoring your hard disk will almost always restore your system, except in the rare cases where the malware resides in your PC's BIOS firmware, in which case you probably need expert help. Unfortunately, the Unified Extensible Firmware Interface (UEFI) adds a new vulnerability as it includes a writable boot partition on your hard disk. Since the code residing here executes before your operating system; any malware

Continued on pg 5

Cont'd from page 4

installed there becomes active before any anti-virus program. Re-installing the operating system will probably leave the infected partition unchanged. So far, this is only a theoretical threat. I mention it only to make the point that threats evolve continuously, which requires that you keep all your software, not just your anti-virus programs updated, and conscientiously practice an effective back up discipline.

To summarize, we can classify computer threats according to their attach method, their behavior, and their payload. Attack methods include physical access to a computer, social engineering, Trojan horse software, and unethical suppliers. Once established, malware can behave as normal software, a rootkit, a virus, a worm, or a combination of these. Typical payloads are ransomware, spyware, key-logger, botnet, and hijacking. Network attacks are special in that they occur outside your computer.Ω

## Interesting Internet Finds – June 2016

Steve Costello, Boca Raton Computer Society
editor@brcs.org
http://ctublog.sefcug.com/

In the course of going through the more than 300 RSS feeds, I often run across things that I think might be of interest to other user group members.

The following are some items I found interesting during the month of June 2016.

*Android Tip: A Faster Way to Launch the Android Camera App*

**http://heresthethingblog.com/2016/06/01/android-tip-faster-launch-camera/**

Quick camera access for Android Marshmallow devices.

*How to Set Up and Use Open365, an Open Source Alternative to Office 365*

http://www.howtogeek.com/256450/how-to-set-up-and-use-open365-an-open-source-alternative-to-office-365/

If you are using LibreOffice, and would like to try out the Open365 (beta at this time) alternative to Office 365, this post from *HowToGeek* is a must read.

*5 Common VPN Myths and Why You Shouldn't Believe Them*

http://www.makeuseof.com/tag/5-common-vpn-myths-shouldnt-believe/

If you don't use a VPN (Virtual Private Network), and you really should, check out this *MakeUseOf* post. Your reason is probably one of these myths.

*Ten Tips for Donating a Computer*

http://www.techsoup.org/support/articles-and-how-tos/ten-tips-for-donating-a-computer

Upgrading to a new computer? Have an unused working computer just laying around? Well check out this post for how best to donate your old computer so someone in need will be able to have one.

*5 Things You Need To Know About Password Managers*

http://www.pcworld.com/article/3085395/security/5-things-you-should-know-about-password-managers.html

I know there a lot of you that don't think you need a password manager. If you are one of them, read this post to learn some reasons why you should.

*Seven Tips on Keeping Your Phone Safe While Traveling*

**http://www.cnet.com/news/seven-tips-on-keeping-your-phone-safe-while-traveling/**

This is the time of year for vacation travel, so check out this post to refresh yourself on how to keep your phone safe while you are out there.**Ω**

## Ransomware - Protecting your ability to recover from an attack

By John Langill, Newsletter Editor, STPCC (Southern Tier Personal Computing Club)
June 2016 issue, Rare Bits

http://www.pageorama.com/?p=stpcc1979jlangil1 (at) stny.rr.com

A recent posting to Yahoo.com reminded me that the key element to recovering from a ransomware attack is to have a reliable system image backup. Most computer users — you among them, I'm sure — are aware of this and have diligently performed regular backups. Some may have chosen to back up their systems to a Cloud-based service for which, if their backup files are sufficiently large, they pay a monthly fee based on the storage

Continued on pg 6

Continued from pg 5

files on a local external hard-drive (never, ever store backup files on an internal hard drive) which one with a three-terabyte capacity, for example, presently costs about $100.

I fall into the latter group.

Cost aside, both methods provide protection but also have their own particular drawbacks that are too often overlooked. What will happen, for instance, if some enterprising ransomware purveyor one day successfully manages to hijack (encrypt) all the client files that have been stored with the cloud-based service. Not possible, such services say. Well, that may be but just how sure of that are you really — or are they, for that matter? And, as sure as God made little green apples, you can bet that there is at least one someone somewhere trying to do just that.

The uncertainty of cloud-based services is what led me to rely on a USB-connected external hard-drive for storing my backup files; and I have been doing so for years with a blissful — and perhaps a false — sense of confidence that they would be secure and uncorrupted should they be needed. Ok, so what's the drawback in this method? The fact is that a ransomware attack will — along with all files stored on the internal hard-drives — also hijack the backup files stored on an external hard-drive unless the drive is either powered off or physically disconnected from the computer at the time of the attack. Not a problem, said I — my USB 3.0 external hard-drive is equipped with an On-Off switch and I power it ON only for the time it takes to create a backup.

There's one other precaution I take and that's to set my cable modem to "Stand by" mode to disrupt Internet traffic during the time that a backup is created; thereby assuring that my system and external hard drives will not be vulnerable to attack while a backup is in progress.

Accordingly, I considered the risk of the backup files becoming corrupted was minimal.

And all was fine and dandy until I decided to swap a relatively low-capacity external hard-drive over to my laptop PC and to install two larger capacity USB 3.0 hard-drives on the desktop PC. The problem with doing this was that the newer drives did not have On-Off switches; and rummaging around behind my desktop PC (which, despite what it's called, is actually located under a desk) to connect and disconnect the USB cables from either the drives themselves or the PC was a real pain — it's a rats-nest back there, as many will probably know.

My solution: I purchased a powered 4-port USB 3.0 hub (under $20) specifically for use with the two newly installed external hard-drives. Now, all I have to do is connect/disconnect the one cable between the hub and the PC. Fortunately, a USB 3.0 port on the front of my PC that makes this convenient and easy. The only thing I need to be careful of is making sure that the external hard-drives have both completed their respective operations before disconnecting the hub from the PC which, by the way, also removes power to the drives (i.e., acts as a defacto power On-Off switch).

Of course, if you use just one external hard-drive to store your backup files, and it has an accessible On-Off switch, you've no problem. Even if the drive doesn't have an ON-Off switch it's likely that restricting Internet access to it will be simply a matter of disconnecting the USB cable from the back of the device and that should not be much of a problem either.

Why do I have two external hard-drives? One is used to directly store backup files — which by the way, are always full system image backups — as they are created. The other serves to archive copies of previously created backups; that is, to back up my backups.

OK, so I'm paranoid when it comes to protecting my system image backups — it's not the worst of my faults. Admittedly, over the past 25 years or so, I can recall only once having to restore a system from a backup. I consider myself lucky on that score. But, with the chance of suffering a malicious attack rapidly increasing at the rate at which it is in today's world — and the risk will only get worse with time — I'd rather be overly cautious than suffer the consequences that result from a lack of vigilance.Ω

**Welcome to**
**NEW MEMBERS!**

**Jeffrey Esslinger**

**Ray Clockel**